CCP Using Metron Dashboard 2.0.1

Using Metron Dashboard

Date of publish: 2017-11-06

https://docs.cloudera.com/

Legal Notice

Contents

Customizing Your Metron Dashboard

You can customize your Metron dashboard to display information, alerts, and the context you need to identify and analyze cybersecurity issues.

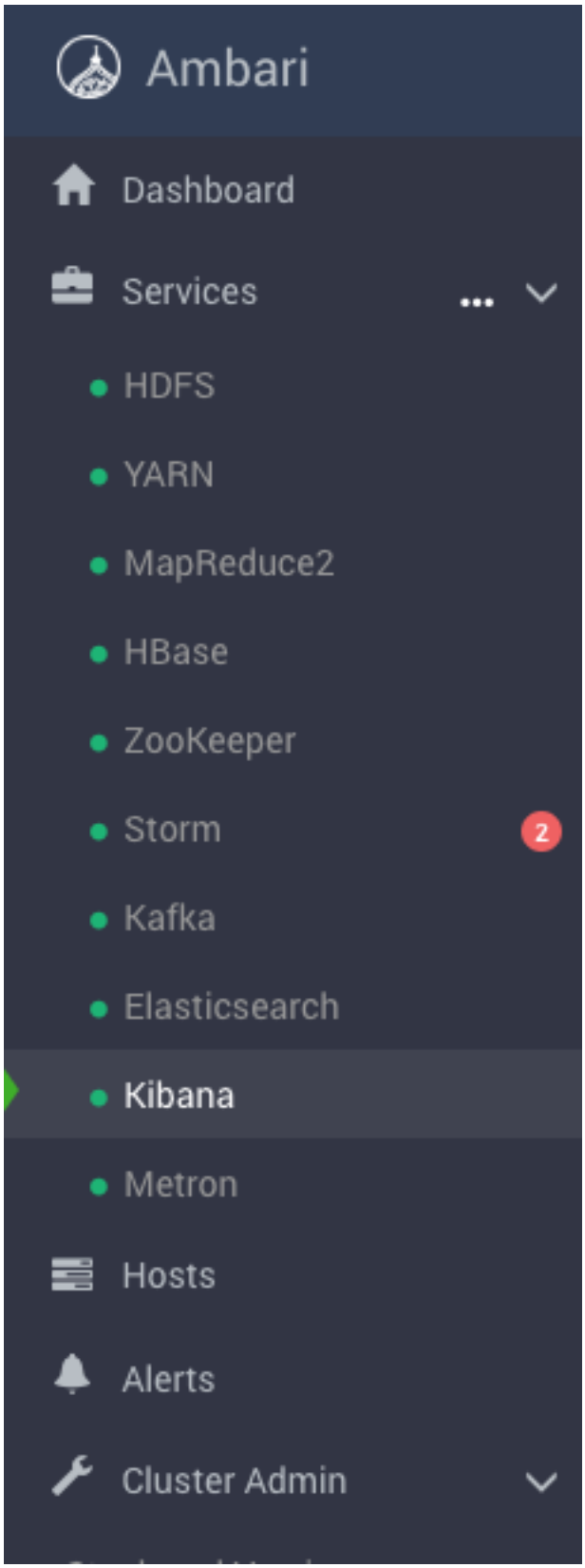
Launching the Metron Dashboard

You can launch the Metron Dashboard using the Ambari UI or a the browser of your choice.

Procedure

1. From Ambari, click Kibana in the list of components.

   Ambari Task List



2. Click **Metron UI** from the **Quick Links** menu.

3. Alternatively, enter the following text in a browser:

```
$KIBANA_HOST:9995
```

Changing the Metron Dashboard Background Color

You can choose to view the Metron dashboard with either a light or dark background. The dark background is sometimes preferred in a dimly lit security operations center.

Procedure

1. Click  (Gear icon) in the top right of the Metron dashboard.

   You should see a check box next to **Use dark theme** near the top of the dashboard.
2. Select the check box to use the dark theme for the dashboard.

   To return to the light theme, clear the check box.

Adding a New Data Source

After a new data telemetry source has been added to CCP, you will need to also add it to the Metron dashboard before you can create queries and filters for it and add telemetry panels displaying its data.

Configuring a New Data Source Index

Now that you have an index for the new data source with all of the right data types, you need to tell the Metron dashboard about this index.

Before you begin

Before you can add a new data telemetry source to the Metron dashboard, you must ensure that you've completed the following steps:

- The data telemetry source must be added to CCP.

  For information on how to add a new data telemetry source, see Prerequisites to Adding a New Telemetry Data Source.
- An index template must be created for the data telemetry source.

  For information on how to create an index template, see Understanding Indexing.

Procedure

To configure your new data source index, see Creating an Index Pattern to Connect to Elasticsearch.

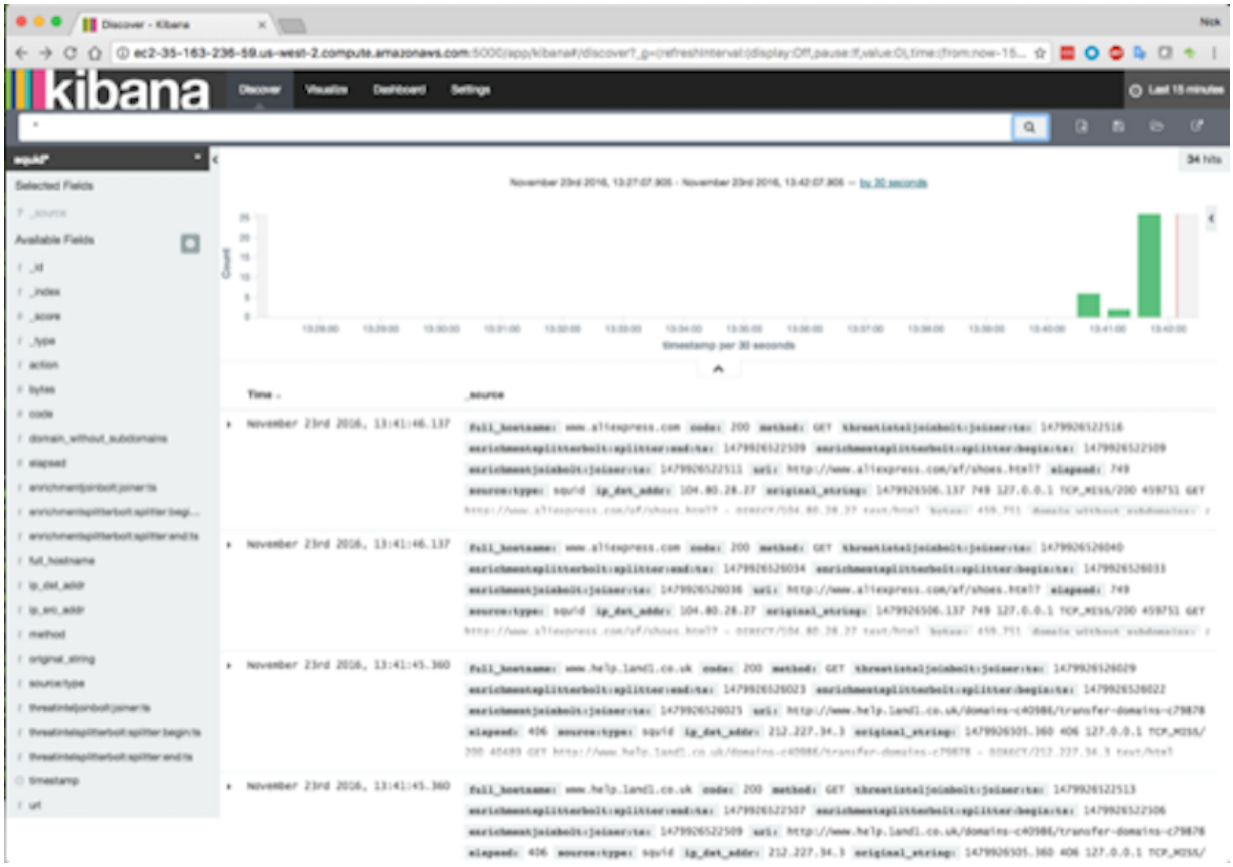
Reviewing the New Data Source Data

Now that the Metron dashboard is aware of the new data source index, you can look at the data.

Procedure

1. Click on the **Discover** tab and then choose the newly created data source index pattern.
2. Click any of the fields in the left column to see a representation of the variety of data for that specific field.
3. Click the Right Facing Arrow icon next to a specific record in the center of the window (the **Document** table) to expand the record and display the available data.

Discover Tab with Squid Elements



Querying, Filtering, and Visualizing Data

You can interactively explore your data source data using the Metron dashboard.

When CCP parses a telemetry, it extracts and normalizes different parts of the message into a standard Metron JSON object. Standardizing and normalizing field names and formats allows CCP to search different telemetry messages with a single query. You have access to every document in every index that matches your selected index patterns. The Metron dashboard enables you to submit search queries on the data source data, filter the search results, and view the results in a number of visualizations.

In CCP, if telemetry indexing is enabled, a rotating index for every telemetry is created. By convention this index will have a name [telemetry_name]_[timestamp]. Telemetry documents indexed into this index will by convention be called [telemetry_name]_doc. Queries reference the document type of the indexed telemetries.

For more information about exploring and analyzing your data, refer to the Kibana documentation:

Table 1: Querying, Filtering, and Visualizing Data

Task	Description	Where to Look
Querying your data	You can search and refine the data you receive from your data source by creating a query from the **Discover** page. You should create and save a query for each data source not provided by CCP. CCP includes queries for the following telemetries: • YAF • Bro • Alerts (populated by Snort) You can also add custom queries for new telemetry types.	Discovering Your Data
Filter your query results	You can use the Metron dashboard to filter your query results to further refine the information. The Metron dashboard provides two types of filters: **Time Filter** — Restricts the search results to a specific time period. **Filter by Field** — Filters to display only those documents that contain a particular value in a field. You can filter either from the Fields list or the Documents table.	Discover
Visualizing your data	You can filter search results to display only those documents that contain a particular value in a field. You can also create negative filters than exclude documents that contain the specified field value.	Visualize

Customizing Your Dashboard

The visualizations in your Metron dashboard are stored in resizeable containers that you can arrange on the dashboard. For more information about customizing your dashboard, see Building a Dashboard.